THE NEED FOR HEALTH PRIVACY PROTECTION BEYOND THE HIPAA PRIVACY RULE

Mark A. Rothstein
Herbert F. Boehl Chair of Law and Medicine
Director, Institute for Bioethics, Health Policy and Law
University of Louisville School of Medicine

It is debatable whether the HIPAA statute and its Privacy Rule ever provided an effective framework for regulating health privacy. It is not debatable that new developments in HIT render the HIPAA Privacy Rule obsolete and incapable of providing meaningful health privacy protection to consumers. Consequently, a new, comprehensive, regulatory approach is necessary, and Congress will need to enact new legislation to provide HHS with the statutory authority to promulgate more far-reaching regulations.

It is well known that health privacy was an afterthought in the HIPAA statute. When Congress added the Administrative Simplification title of HIPAA, thereby committing the nation to electronic processing of health claims, Congress also committed to protecting the privacy and security of health information. Unable to enact statutory health privacy protection by its self-imposed deadline, the responsibility was assigned to the Secretary of HHS. The resulting HIPAA Privacy Rule, designed to protect health privacy in the health payment chain, was never intended to have comprehensive scope. By statute, HIPAA coverage is limited to certain health care providers, health plans, and health clearinghouses.

Not all health care providers are subject to the Privacy Rule. Tens of thousands of providers that deal with individually-identifiable health information are not subject to HIPAA because they do not submit electronic claims for payment. This includes numerous providers whose services are rendered without charge (e.g., mental health counselors and social workers provided by a social service agency, employer-supplied occupational health clinics) or who receive payment in cash (e.g., some "concierge" medical practices, massage therapists, cosmetic medicine practices, urgent care facilities, home testing laboratories, health and fitness clubs, and "alternative" medicine providers).

A health care provider's legal obligation to protect the privacy of personal health information should not turn on whether or how the provider is paid. The harm to be avoided has nothing to do with the method of payment, and individuals' health privacy should not vary based on the irrelevant criterion of method of claims processing. Furthermore, members of the public are already confused about the extent of protection

of their health information, and they should not be put in the position of relying – perhaps to their detriment – on a federal rule of limited applicability.

The Privacy Rule also does not apply to numerous non-health care entities that routinely receive and consider information contained in individually-identifiable health records. These entities include employers, life insurers, disability insurers, long-term care insurers, financial institutions, and other public and private entities. In some instances, the disclosures of health information are permitted without any consent or authorization (e.g., disclosures to public health authorities); in other instances, individuals are "compelled" to execute an authorization if they want to apply for a job or insurance. Once information is released to third parties that are not covered entities, HIPAA does not apply to any subsequent uses and disclosures.

It has been only 11 years since HIPAA was enacted, but in this short time the world of HIT has been transformed. An entire new industry is rapidly emerging to foster the exchange of electronic health information. HIEs, RHIOs, medical record banks, PHR vendors, and other entities are usually not directly covered by the Privacy Rule. Some of these entities may be business associates of covered entities and therefore may be required to be HIPAA compliant. The level of privacy protection maintained by business associates of covered entities, however, may be seriously questioned. Besides receiving an initial notice of privacy practices, individuals are not entitled to a specific notice that a business associate agreement has been executed or to the specific provisions of the agreement. Business associates also may subcontract their responsibilities to other entities, including overseas entities, over which there may be even less supervision and control. In effect, responsibility for the privacy and confidentiality of personally-identifiable health information may be delegated to private parties and overseen by other private parties.

Business associate arrangements are also plagued by a lack of effective enforcement. Entities with only "indirect" HIPAA duties are subject only to contract claims brought by the covered entity, and they are not subject to enforcement actions by HHS or DOJ. Moreover, it is arguable that the HHS policy of conciliation rather than enforcement in response to HIPAA Privacy Rule complaints filed with OCR fails to encourage covered entities to closely monitor the privacy practices of their business associates.

Although the lack of coverage of business associates is a significant problem under the HIPAA Privacy Rule, it is not the only shortcoming. In contemplating the effect of the Privacy Rule on the post-NHIN world of electronic health information exchange, the five following shortcomings also deserve mention: (1) under HIPAA, individuals are entitled only to receive an NPP, they are not given an opportunity to opt-in or opt-out of a network, a key requirement for such an expanded aggregation of their health information; (2) under HIPAA, patients have no ability to segregate sensitive elements of their health records, such as by having separate restrictions on disclosure of substance abuse, mental health, reproductive health, or other information; (3) under HIPAA, there are no provisions for establishing contextual access criteria or role-based

access criteria to restrict the scope of disclosures; (4) under HIPAA, there are loose standards for the disclosure of PHI to law enforcement and other third party requestors that are even more problemmatic in the context of disclosing an individual's complete, cradle-to-grave health records; and (5) under HIPAA, there is inadequate enforcement, research, oversight, outreach, and education.

The NHIN will facilitate the development of interoperable networks of EHRs. In turn, these networks will enable the disclosure of significantly greater quantities of longitudinal and comprehensive health information. The greater volume of health information subject to disclosure increases the likelihood that individual health records will contain sensitive material. Consequently, it is extremely important to develop and impliment strict privacy and security rules for the NHIN. (Although it is beyond the scope of this comment, privacy- and security-enhancing provisions also need to be incorporated into the architecture and infrastructure of the NHIN.) Without these protections, both in the letter of the law and in the aggressive enforcement of the law, members of the public will lack the trust to participate with confidence in the NHIN.

In a real sense, the shortcomings of the HIPAA Privacy Rule will be magnified with the establishment of the NHIN. The foremost shortcoming of HIPAA is its limited applicability. If Congress fails to address this fundamental issue, all of the other needed revisions of the Privacy Rule will be largely irrelevant. Comprehensive health information exchange demands comprehensive privacy and security protection.